T S6/5/1

6/5/1
DIALOG(R)File 351:Derwent WPI

013608276
WPI Acc No: 2001-092484/200111
XRPX Acc No: N01-069981
Electronic storage device for guaranteeing originality of electronic data varies level of access based on if data are original data or not
Patent Assignee: RICOH KK (RICO)
Inventor: KANAI Y; YACHIDA M
Number of Countries: 002 Number of Patents: 007
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
DE 10024753	A1	20001221	DE 1024753	A	20000519	200111	B
JP 2000339223	A	20001208	JP 99145340	A	19990525	200113	
JP 2001005728	A	20010112	JP 99173371	A	19990618	200118	
JP 2001147898	A	20010529	JP 99328802	A	19991118	200136	
JP 2001154577	A	20010608	JP 99338741	A	19991129	200138	
JP 2001209582	A	20010803	JP 200015092	A	20000124	200150	
JP 2001209581	A	20010803	JP 200015091	A	20000124	200150	

Priority Applications (No Type Date): JP 200015092 A 20000124; JP 99145340 A 19990525; JP 99173371 A 19990618; JP 99328802 A 19991118; JP 99338741 A 19991129; JP 200015091 A 20000124
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
DE 10024753	A1		159	G06F-012/14	
JP 2000339223	A		29	G06F-012/14	
JP 2001005728	A		46	G06F-012/14	
JP 2001147898	A		11	G06F-015/00	
JP 2001154577	A		12	G09C-001/00	
JP 2001209582	A		18	G06F-012/14	
JP 2001209581	A		16	G06F-012/14	

Abstract (Basic): DE 10024753 A1

NOVELTY - The storage device includes a storage unit which stores electronic data consisting of a number of content files as a single original in an identifiable state. An access unit controls the access to the original electronic data at a level which is different from the level of access to non-original electronic data. The storage unit stores tamper detection information as original information corresponding to the electronic data.

DETAILED DESCRIPTION - The storage device may include a tamper detection information computing device which receives a request to re-store the electronic data as a single original using an encryption key to compute tamper detection information for each of the content files. A second tamper detection information computing device uses the encryption key to compute second temper detection information for edition management information. INDEPENDENT CLAIMS are included for an electronic storage device, an authorization verification system, an electronic storage method, an authorization verification method, damage recovery method and a storage medium for storing a program in a computer.

USE - For originality-guarantee electronic preservation systems using large-capacity storage media.

ADVANTAGE - Allows the originality of a combined document comprising multiple files to be guaranteed.

pp; 159 DwgNo 0/74
Title Terms: ELECTRONIC; STORAGE; DEVICE; GUARANTEE; ELECTRONIC; DATA; VARY ; LEVEL; ACCESS; BASED; DATA; ORIGINAL; DATA
Derwent Class: P85; T01
International Patent Class (Main): G06F-012/14; G06F-015/00
International Patent Class (Additional): G06F-003/06; G06F-009/06; G06F-012/00; G06F-012/16; G06F-017/30; G06F-017/60; G09C-001/00
File Segment: EPI; EngPI
?

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2001－209581
（P2001－209581A）
(43)公開日　平成13年８月３日(2001.8.3)

(51)Int.Cl.'	識別記号	ＦＩ	ﾃｰﾏｺｰﾄﾞ(参考)
Ｇ０６Ｆ　12/14	３１０	Ｇ０６Ｆ　12/14	３１０Ｚ　５Ｂ０１７

審査請求　未請求　請求項の数15　ＯＬ　（全 16 頁）

(21)出願番号　特願2000－15091(P2000－15091)

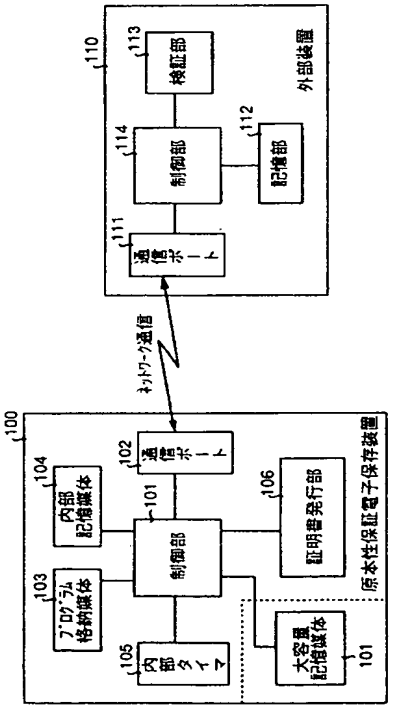
(22)出願日　平成12年１月24日(2000.1.24)

(71)出願人　000006747
株式会社リコー
東京都大田区中馬込１丁目３番６号
(72)発明者　金井　洋一
東京都大田区中馬込１丁目３番６号　株式会社リコー内
(72)発明者　谷内田　益義
東京都大田区中馬込１丁目３番６号　株式会社リコー内
(74)代理人　100104190
弁理士　酒井　昭徳

Ｆターム(参考)　5B017 AA06 AA08 BA05 BA07 BB02
BB10 CA09 CA16

(54)【発明の名称】　正当性検証システム、正当性検証方法およびその方法をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体

(57)【要約】
【課題】　原本性保証電子保存装置以外の装置上に原本のコピーを保持する場合に、このコピーが原本の保存データと一致することを効率良く保証すること。
【解決手段】　原本性保証電子保存装置１０６の証明書発行部１０６が原本をコピーした複写データについての保存証明書を発行し、外部装置１１０の検証部１１３が保存証明書に基づいて複写データの正当性を検証する。



1

【特許請求の範囲】

【請求項１】　所定の記憶部に記憶した原本データを複写した複写データの正当性を検証する正当性検証システムにおいて、

前記複写データが前記原本データとその内容が一致することを証明する証明書を発行する証明書発行手段と、

前記証明書発行手段により発行された証明書に基づいて、前記複写データの正当性を検証する検証手段と、

を備えたことを特徴とする正当性検証システム。

【請求項２】　前記証明書発行手段は、

前記記憶部に記憶した前記原本データについての第１のハッシュ値を算定する第１のハッシュ値算定手段と、

前記第１のハッシュ値算定手段により算定された第１のハッシュ値を所定の秘密鍵で暗号化する暗号化手段と、

前記暗号化手段により暗号化された暗号データを証明書として出力する証明書出力手段と、

を備えたことを特徴とする請求項１に記載の正当性検証システム。

【請求項３】　前記証明書発行手段は、

前記原本データについての第１のハッシュ値を算定する第１のハッシュ値算定手段と、

前記第１のハッシュ値算定手段により算定された第１のハッシュ値、現在時刻および前記原本データの識別情報を含む証明内容を作成する証明内容作成手段と、

前記証明内容作成手段により作成された証明内容についての第２のハッシュ値を算定する第２のハッシュ値算定手段と、

前記第２のハッシュ値算定手段により算定された第２のハッシュ値並びに前記証明内容作成手段により作成された証明内容からなる証明書を出力する証明書出力手段と、

を備えたことを特徴とする請求項１に記載の正当性検証システム。

【請求項４】　前記第１のハッシュ値算定手段は、前記記憶部に記憶した原本データの最新版の内容データとその属性情報についての第１のハッシュ値を算定することを特徴とする請求項３に記載の正当性検証システム。

【請求項５】　前記検証手段は、

前記証明書発行手段により発行された証明書とともに検証要求を受け付けた際に、当該証明書を前記秘密鍵に対応する公開鍵で復号化する復号化手段と、

前記所定の記憶部に記憶した原本データのハッシュ値を算定するハッシュ値算定手段と、

前記算定手段により算定されたハッシュ値および前記復号化手段により復号化された値を比較して、両者が一致する場合にのみ前記複写データが正当であるものと判定する判定手段と、

を備えたことを特徴とする請求項２に記載の正当性検証システム。

【請求項６】　前記検証手段は、

2

前記証明書に含まれる前記第２のハッシュ値を前記秘密鍵に対応する公開鍵で復号化する復号化手段と、

前記証明書に含まれる証明内容についての第３のハッシュ値を算定する第３のハッシュ値算定手段と、

前記復号化手段により復号化された第２のハッシュ値および前記第３のハッシュ値算定手段により算定された第３のハッシュ値が一致する場合に、前記証明内容に含まれる識別情報に対応する原本データを前記記憶部から読み出す読出手段と、

前記読出手段により読み出された原本データについての第４のハッシュ値を算定する第４のハッシュ値算定手段と、

前記第４のハッシュ値算定手段により算定された第４のハッシュ値および前記証明内容に含まれる第１のハッシュ値を比較して、両者が一致する場合にのみ前記複写データが正当であるものと判定する判定手段と、

を備えたことを特徴とする請求項３に記載の正当性検証システム。

【請求項７】　前記第４のハッシュ値算定手段は、前記読出手段により読み出された原本データの最新版の内容データとその属性情報についての第４のハッシュ値を算定することを特徴とする請求項６に記載の正当性検証システム。

【請求項８】　所定の記憶部に記憶した原本データを複写した複写データの正当性を検証する正当性検証方法において、

前記複写データが前記原本データとその内容が一致することを証明する証明書を発行する証明書発行工程と、

前記証明書発行工程により発行された証明書に基づいて、前記複写データの正当性を検証する検証工程と、

を含んだことを特徴とする正当性検証方法。

【請求項９】　前記証明書発行工程は、

前記記憶部に記憶した前記原本データについての第１のハッシュ値を算定する第１のハッシュ値算定工程と、

前記第１のハッシュ値算定工程により算定された第１のハッシュ値を所定の秘密鍵で暗号化する暗号化工程と、

前記暗号化工程により暗号化された暗号データを証明書として出力する証明書出力工程と、

を含んだことを特徴とする請求項８に記載の正当性検証方法。

【請求項１０】　前記証明書発行工程は、

前記原本データについての第１のハッシュ値を算定する第１のハッシュ値算定工程と、

前記第１のハッシュ値算定工程により算定された第１のハッシュ値、現在時刻および前記原本データの識別情報を含む証明内容を作成する証明内容作成工程と、

前記証明内容作成工程により作成された証明内容についての第２のハッシュ値を算定する第２のハッシュ値算定工程と、

前記第２のハッシュ値算定工程により算定された第２の

ハッシュ値並びに前記証明内容作成工程により作成された証明内容からなる証明書を出力する証明書出力工程と、

を含んだことを特徴とする請求項８に記載の正当性検証方法。

【請求項１１】　前記第１のハッシュ値算定工程は、前記記憶部に記憶した原本データの最新版の内容データとその属性情報についての第１のハッシュ値を算定することを特徴とする請求項１０に記載の正当性検証方法。

【請求項１２】　前記検証工程は、

前記証明書発行工程により発行された証明書とともに検証要求を受け付けた際に、当該証明書を前記秘密鍵に対応する公開鍵で復号化する復号化工程と、

前記所定の記憶部に記憶した原本データのハッシュ値を算定するハッシュ値算定工程と、

前記算定工程により算定されたハッシュ値および前記復号化工程により復号化された値を比較して、両者が一致する場合にのみ前記複写データが正当であるものと判定する判定工程と、

を含んだことを特徴とする請求項９に記載の正当性検証方法。

【請求項１３】　前記検証工程は、

前記証明書に含まれる前記第２のハッシュ値を前記秘密鍵に対応する公開鍵で復号化する復号化工程と、

前記証明書に含まれる証明内容についての第３のハッシュ値を算定する第３のハッシュ値算定工程と、

前記復号化工程により復号化された第２のハッシュ値および前記第３のハッシュ値算定工程により算定された第３のハッシュ値が一致する場合に、前記証明内容に含まれる識別情報に対応する原本データを前記記憶部から読み出す読出工程と、

前記読出工程により読み出された原本データについての第４のハッシュ値を算定する第４のハッシュ値算定工程と、

前記第４のハッシュ値算定工程により算定された第４のハッシュ値および前記証明内容に含まれる第１のハッシュ値とを比較して、両者が一致する場合にのみ前記複写データが正当であるものと判定する判定工程と、

を含んだことを特徴とする請求項１０に記載の正当性検証方法。

【請求項１４】　前記第４のハッシュ値算定工程は、前記読出工程により読み出された原本データの最新版の内容データとその属性情報についての第４のハッシュ値を算定することを特徴とする請求項１３に記載の正当性検証方法。

【請求項１５】　前記請求項８～１４のいずれか一つに記載された方法をコンピュータに実行させるプログラムを記録したことを特徴とするコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、所定の記憶部に記憶した原本データを複写した複写データの正当性を検証する正当性検証システム、正当性検証方法およびその方法をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体に関し、特に、原本性保証電子保存装置以外の装置上に原本のコピーを保持する場合に、このコピーが原本の保存データと一致することを効率良く保証することができる正当性検証システム、正当性検証方法および記録媒体に関する。

【０００２】

【従来の技術】近年のコンピュータ技術の進展に伴うペーパーレス化の進展に伴って、紙によって原本書類として保存されていた情報が電子データの形式で保存される場合が増えてきたため、かかる電子データの原本性を保証する従来技術が知られている。

【０００３】たとえば、「金井他：原本性保証電子保存システムの開発－システムの構築－，Medical Imaging Tecnology, Vol.16, No.4, Proceedings of JAMIT Annual Meeting'98(1998)」や、「国分他：原本性保証電子保存システムの開発，（特）情報処理振興事業協会発行　創造的ソフトウエア育成事業およびエレクトロニック・コマース推進事業　最終成果発表会論文集　創造的ソフトウエア育成事業編(1998)」には、電子データの原本性を保証するシステムの一例が開示されている。

【０００４】かかる従来技術を用いると、電子データの原本性を保証することが可能となり、これにより原本書類を電子データの形式で保存し、もって高度情報化社会の推進並びに社会全体の生産性向上に寄与することができる。

【０００５】

【発明が解決しようとする課題】しかしながら、これらの従来技術は、あくまでも原本性保証電子保存装置内部で管理されている保存データの原本性を保証するものでしかないので、そのコピーを作成して外部の装置上に保持する際に、このコピーが原本の保存データと本当に一致するか否かを効率良く保証することができないという問題がある。

【０００６】すなわち、原本性保証電子保存装置以外の装置上に原本のコピーを保持する場合には、このコピーとともに原本の保存データについても当該装置上に移動しなければ、該コピーと原本の保存データが一致するか否かを調べることができないこととなる。

【０００７】ここで、本来原本としての保存データは、原本性保証電子保存装置上にのみ保持すべきであり、様々な装置上を移動させることとしたのでは、原本の保存データの喪失や原本の保存データの改ざんを招く機会を与えることとなるので、妥当ではない。なお、原本を移動する代わりに原本のコピーを移動することも考えられるが、原本の保存データをコピーしたものはすでに原本

とは言えない。

【０００８】これらのことから、原本性保証電子保存装置以外の装置上に原本のコピーを保持する場合に、このコピーが原本の保存データと一致することをいかに効率良く検証するかが極めて重要な課題となっている。

【０００９】この発明は、上記問題（課題）に鑑みてなされたものであり、原本性保証電子保存装置以外の装置上に原本のコピーを保持する場合に、このコピーが原本の保存データと一致することを効率良く保証することができる原本性保証電子保存システム、正当性保証方法および記録媒体を提供することを目的とする。

【００１０】

【課題を解決するための手段】上記目的を達成するために、請求項１に記載の発明にかかる正当性検証システムは、所定の記憶部に記憶した原本データを複写した複写データの正当性を検証する正当性検証システムにおいて、前記複写データが前記原本データとその内容が一致することを証明する証明書を発行する証明書発行手段と、前記証明書発行手段により発行された証明書に基づいて、前記複写データの正当性を検証する検証手段と、を備えたことを特徴とする。

【００１１】この請求項１に記載の発明によれば、複写データが原本データとその内容が一致することを証明する証明書を発行し、発行した証明書に基づいて複写データの正当性を検証することとしたので、原本性保証電子保存装置以外の装置上に原本のコピーを保持する場合に、このコピーが原本の保存データと一致することを効率良く保証することができる。

【００１２】また、請求項２に記載の発明にかかる正当性検証システムは、請求項１に記載の発明において、前記証明書発行手段は、前記記憶部に記憶した前記原本データについての第１のハッシュ値を算定する第１のハッシュ値算定手段と、前記第１のハッシュ値算定手段により算定された第１のハッシュ値を所定の秘密鍵で暗号化する暗号化手段と、前記暗号化手段により暗号化された暗号データを証明書として出力する証明書出力手段と、を備えたことを特徴とする。

【００１３】この請求項２に記載の発明によれば、記憶部に記憶した原本データについての第１のハッシュ値を算定し、算定した第１のハッシュ値を所定の秘密鍵で暗号化し、暗号化した暗号データを証明書として出力することとしたので、迅速かつ効率良く証明書を発行することができる。

【００１４】また、請求項３に記載の発明にかかる正当性検証システムは、請求項１に記載の発明において、前記証明書発行手段は、前記原本データについての第１のハッシュ値を算定する第１のハッシュ値算定手段と、前記第１のハッシュ値算定手段により算定された第１のハッシュ値、現在時刻および前記原本データの識別情報を含む証明内容を作成する証明内容作成手段と、前記証明内容作成手段により作成された証明内容についての第２のハッシュ値を算定する第２のハッシュ値算定手段と、前記第２のハッシュ値算定手段により算定された第２のハッシュ値並びに前記証明内容作成手段により作成された証明内容からなる証明書を出力する証明書出力手段と、を備えたことを特徴とする。

【００１５】この請求項３に記載の発明によれば、原本データについての第１のハッシュ値を算定し、算定した第１のハッシュ値、現在時刻および原本データの識別情報を含む証明内容を作成し、作成した証明内容についての第２のハッシュ値を算定し、算定した第２のハッシュ値並びに証明内容からなる証明書を出力することとしたので、２重にハッシュ化した高い正当性を保証することができる証明書を発行することができる。

【００１６】また、請求項４に記載の発明にかかる正当性検証システムは、請求項３に記載の発明において、前記第１のハッシュ値算定手段は、前記記憶部に記憶した原本データの最新版の内容データとその属性情報についての第１のハッシュ値を算定することを特徴とする。

【００１７】この請求項４に記載の発明によれば、記憶部に記憶した原本データの最新版の内容データとその属性情報についての第１のハッシュ値を算定することとしたので、正当性を保証すべき内容のみに限定した保証書を効率良く発行することができる。

【００１８】また、請求項５に記載の発明にかかる正当性検証システムは、請求項２に記載の発明において、前記検証手段は、前記証明書発行手段により発行された証明書とともに検証要求を受け付けた際に、当該証明書を前記秘密鍵に対応する公開鍵で復号化する復号化手段と、前記所定の記憶部に記憶した原本データのハッシュ値を算定するハッシュ値算定手段と、前記算定手段により算定されたハッシュ値および前記復号化手段により復号化された値を比較して、両者が一致する場合にのみ前記複写データが正当であるものと判定する判定手段と、を備えたことを特徴とする。

【００１９】この請求項５に記載の発明によれば、発行された証明書とともに検証要求を受け付けた際に、当該証明書を秘密鍵に対応する公開鍵で復号化するとともに、記憶部に記憶した原本データのハッシュ値を算定し、算定したハッシュ値および復号化された値を比較して、両者が一致する場合にのみ複写データが正当であるものと判定することとしたので、迅速かつ効率良く複写データの正当性を検証することができる。

【００２０】また、請求項６に記載の発明にかかる正当性検証システムは、請求項３に記載の発明において、前記検証手段は、前記証明書に含まれる前記第２のハッシュ値を前記秘密鍵に対応する公開鍵で復号化する復号化手段と、前記証明書に含まれる証明内容についての第３のハッシュ値を算定する第３のハッシュ値算定手段と、前記復号化手段により復号化された第２のハッシュ値お

よび前記第３のハッシュ値算定手段により算定された第３のハッシュ値が一致する場合に、前記証明内容に含まれる識別情報に対応する原本データを前記記憶部から読み出す読出手段と、前記読出手段により読み出された原本データについての第４のハッシュ値を算定する第４のハッシュ値算定手段と、前記第４のハッシュ値算定手段により算定された第４のハッシュ値および前記証明内容に含まれる第１のハッシュ値とを比較して、両者が一致する場合にのみ前記複写データが正当であるものと判定する判定手段と、を備えたことを特徴とする。

【００２１】この請求項６に記載の発明によれば、証明書に含まれる第２のハッシュ値を秘密鍵に対応する公開鍵で復号化するとともに、証明書に含まれる証明内容についての第３のハッシュ値を算定し、この復号化された第２のハッシュ値および算定された第３のハッシュ値が一致する場合に、証明内容に含まれる識別情報に対応する原本データを記憶部から読み出し、読み出した原本データについての第４のハッシュ値を算定し、算定した第４のハッシュ値および証明内容に含まれる第１のハッシュ値を比較して、両者が一致する場合にのみ複写データが正当であるものと判定することとしたので、より確実に複写データが正当なものであるか否かを検証することができる。

【００２２】また、請求項７に記載の発明にかかる正当性検証システムは、請求項６に記載の発明において、前記第４のハッシュ値算定手段は、前記読出手段により読み出された原本データの最新版の内容データとその属性情報についての第４のハッシュ値を算定することを特徴とする。

【００２３】この請求項７に記載の発明によれば、読み出された原本データの最新版の内容データとその属性情報についての第４のハッシュ値を算定することとしたので、検証時間の短縮化を図ることができる。

【００２４】また、請求項８に記載の発明にかかる正当性検証方法は、所定の記憶部に記憶した原本データを複写した複写データの正当性を検証する正当性検証方法において、前記複写データが前記原本データとその内容が一致することを証明する証明書を発行する証明書発行工程と、前記証明書発行工程により発行された証明書に基づいて、前記複写データの正当性を検証する検証工程と、を含んだことを特徴とする。

【００２５】この請求項８に記載の発明によれば、複写データが原本データとその内容が一致することを証明する証明書を発行し、発行した証明書に基づいて複写データの正当性を検証することとしたので、原本性保証電子保存装置以外の装置上に原本のコピーを保持する場合に、このコピーが原本の保存データと一致することを効率良く保証することができる。

【００２６】また、請求項９に記載の発明にかかる正当性検証方法は、請求項８に記載の発明において、前記証明書発行工程は、前記記憶部に記憶した前記原本データについての第１のハッシュ値を算定する第１のハッシュ値算定工程と、前記第１のハッシュ値算定工程により算定された第１のハッシュ値を所定の秘密鍵で暗号化する暗号化工程と、前記暗号化工程により暗号化された暗号データを証明書として出力する証明書出力工程と、を含んだことを特徴とする。

【００２７】この請求項９に記載の発明によれば、記憶部に記憶した原本データについての第１のハッシュ値を算定し、算定した第１のハッシュ値を所定の秘密鍵で暗号化し、暗号化した暗号データを証明書として出力することとしたので、迅速かつ効率良く証明書を発行することができる。

【００２８】また、請求項１０に記載の発明にかかる正当性検証方法は、請求項８に記載の発明において、前記証明書発行工程は、前記原本データについての第１のハッシュ値を算定する第１のハッシュ値算定工程と、前記第１のハッシュ値算定工程により算定された第１のハッシュ値、現在時刻および前記原本データの識別情報を含む証明内容を作成する証明内容作成工程と、前記証明内容作成工程により作成された証明内容についての第２のハッシュ値を算定する第２のハッシュ値算定工程と、前記第２のハッシュ値算定工程により算定された第２のハッシュ値並びに前記証明内容作成工程により作成された証明内容からなる証明書を出力する証明書出力工程と、を含んだことを特徴とする。

【００２９】この請求項１０に記載の発明によれば、原本データについての第１のハッシュ値を算定し、算定した第１のハッシュ値、現在時刻および原本データの識別情報を含む証明内容を作成し、作成した証明内容についての第２のハッシュ値を算定し、算定した第２のハッシュ値並びに証明内容からなる証明書を出力することとしたので、２重にハッシュ化した高い正当性を保証することができる証明書を発行することができる。

【００３０】また、請求項１１に記載の発明にかかる正当性検証方法は、請求項１０に記載の発明において、前記第１のハッシュ値算定工程は、前記記憶部に記憶した原本データの最新版の内容データとその属性情報についての第１のハッシュ値を算定することを特徴とする。

【００３１】この請求項１１に記載の発明によれば、記憶部に記憶した原本データの最新版の内容データとその属性情報についての第１のハッシュ値を算定することとしたので、正当性を保証すべき内容のみに限定した保証書を効率良く発行することができる。

【００３２】また、請求項１２に記載の発明にかかる正当性検証方法は、請求項９に記載の発明において、前記検証工程は、前記証明書発行工程により発行された証明書とともに検証要求を受け付けた際に、当該証明書を前記秘密鍵に対応する公開鍵で復号化する復号化工程と、前記所定の記憶部に記憶した原本データのハッシュ値を

算定するハッシュ値算定工程と、前記算定工程により算定されたハッシュ値および前記復号化工程により復号化された値を比較して、両者が一致する場合にのみ前記複写データが正当であるものと判定する判定工程と、を含んだことを特徴とする。

【００３３】この請求項１２に記載の発明によれば、発行された証明書とともに検証要求を受け付けた際に、当該証明書を秘密鍵に対応する公開鍵で復号化するとともに、記憶部に記憶した原本データのハッシュ値を算定し、算定したハッシュ値および復号化された値を比較して、両者が一致する場合にのみ複写データが正当であるものと判定することとしたので、迅速かつ効率良く複写データの正当性を検証することができる。

【００３４】また、請求項１３に記載の発明にかかる正当性検証方法は、請求項１０に記載の発明において、前記検証工程は、前記証明書に含まれる前記第２のハッシュ値を前記秘密鍵に対応する公開鍵で復号化する復号化工程と、前記証明書に含まれる証明内容についての第３のハッシュ値を算定する第３のハッシュ値算定工程と、前記復号化工程により復号化された第２のハッシュ値および前記第３のハッシュ値算定工程により算定された第３のハッシュ値が一致する場合に、前記証明内容に含まれる識別情報に対応する原本データを前記記憶部から読み出す読出工程と、前記読出工程により読み出された原本データについての第４のハッシュ値を算定する第４のハッシュ値算定工程と、前記第４のハッシュ値算定工程により算定された第４のハッシュ値および前記証明内容に含まれる第１のハッシュ値とを比較して、両者が一致する場合にのみ前記複写データが正当であるものと判定する判定工程と、を含んだことを特徴とする。

【００３５】この請求項１３に記載の発明によれば、証明書に含まれる第２のハッシュ値を秘密鍵に対応する公開鍵で復号化するとともに、証明書に含まれる証明内容についての第３のハッシュ値を算定し、この復号化された第２のハッシュ値および算定された第３のハッシュ値が一致する場合に、証明内容に含まれる識別情報に対応する原本データを記憶部から読み出し、読み出した原本データについての第４のハッシュ値を算定し、算定した第４のハッシュ値および証明内容に含まれる第１のハッシュ値を比較して、両者が一致する場合にのみ複写データが正当であるものと判定することとしたので、より確実に複写データが正当なものであるか否かを検証することができる。

【００３６】また、請求項１４に記載の発明にかかる正当性検証方法は、請求項１３に記載の発明において、前記第４のハッシュ値算定工程は、前記読出工程により読み出された原本データの最新版の内容データとその属性情報についての第４のハッシュ値を算定することを特徴とする。

【００３７】この請求項１４に記載の発明によれば、読み出された原本データの最新版の内容データとその属性情報についての第４のハッシュ値を算定することとしたので、検証時間の短縮化を図ることができる。

【００３８】また、請求項１５に記載の発明にかかる記録媒体は、前記請求項８～１４のいずれか一つに記載された方法をコンピュータに実行させるプログラムを記録したことで、そのプログラムが機械読み取り可能となり、これによって、請求項８～１４の動作をコンピュータによって実現することができる。

【００３９】

【発明の実施の形態】以下に添付図面を参照して、この発明にかかる正当性検証システム、正当性検証方法およびその方法をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体の好適な実施の形態を詳細に説明する。

【００４０】図１は、本実施の形態で用いる正当性検証システムのシステム構成を示すブロック図である。同図に示す正当性検証システムは、原本の保存データを保持する原本性保証電子保存装置１００と、この原本の保存データのコピーを原本性保証電子保存装置１００から受け取る外部装置１１０とをネットワークで接続したものである。

【００４１】すなわち、この正当性検証システムでは、原本性保証電子保存装置１００が大容量記憶媒体１０１上に保持する原本のコピーを作成する際に、このコピーが原本と同一であることを検証できる保存証明書を発行し、これにより外部装置１１０上でコピーの正当性を検証できるようにしている。

【００４２】同図に示すように、原本性保証電子保存装置１００は、大容量記憶媒体１０１と、通信ポート１０２と、プログラム格納媒体１０３と、内部記憶媒体１０４と、内部タイマ１０５と、証明書発行部１０６と、制御部１０７とからなる。

【００４３】大容量記憶媒体１０１は、原本となる電子データなどを記憶する大容量の二次記憶装置であり、たとえば光磁気ディスクやＣＤ－Ｒなどからなる。通信ポート１０２は、ネットワークを介して外部装置１１０との通信をおこなうためのインターフェース部であり、たとえばＬＡＮカードなどの通信モデムなどからなる。

【００４４】プログラム格納媒体１０３は、主制御プログラム、ハッシュプログラム、鍵生成プログラム、暗号化プログラムおよび復号化プログラムなどの各種プログラムを格納したメモリであり、たとえば書換可能なＥＥＰＲＯＭや読み出し専用のＲＯＭなどからなる。

【００４５】内部記憶媒体１０４は、各種プログラムの実行に必要となるパラメータを記憶するＥＥＰＲＯＭなどからなるメモリであり、具体的には、装置暗号鍵、装置復号鍵、媒体認証コードリスト、最新データ識別番号、タイマ設定履歴ファイルおよびアカウント管理リストなどを記憶する。内部タイマ１０５は、制御部１０７

の本体をなすプロセッサ１０６がプログラムの実行時に所得する時刻を計時するタイマである。

【００４６】証明書発行部１０６は、原本性保証電子保存装置１００が大容量記憶媒体１０１上に保持する原本のコピーを作成した場合に、外部装置１１０からの要求に基づいてこのコピーが原本と同一であることを検証できる保存証明書を発行する処理部である。

【００４７】具体的には、原本の保存データは、データ属性ファイル、データアクセス履歴ファイル、データ認証ファイルおよびコンテンツファイルにより形成されるが、このうち外部装置にコピーを作成する対象となるのは、基本的に最新バージョンの状態（属性情報含む）だけであり、アクセス履歴についてまで外部にコピーを作成する必要はないので、この証明書発行部１０６は、コンテンツファイルのうちの最新バージョンに相当するファイルと、データ属性情報のみを対象として保存証明書を作成する。

【００４８】なお、大容量記憶媒体１０１については、図中に破線で示したように原本性保証電子保存装置１００から取り外し可能としても良いが、その他の構成部位については原本性保証電子保存装置１００と物理的に一体化し、通信ポート１０２以外からのアクセスを受け付けない耐タンパー性を有する構成にする。

【００４９】ただし、この耐タンパー性には、筐体を開けられないようにシールを貼る程度のレベルから、筐体を開けた場合に装置が動作しなくなるレベルまで様々なものがあるが、本発明はこの耐タンパー性のレベルには特段の制限を受けない。

【００５０】制御部１０７は、その実体はプロセッサであり、プログラム格納媒体１０３に格納された主制御プログラム、ハッシュプログラム、鍵生成プログラム、暗号化プログラムおよび復号化プログラムなどの各種プログラムを読み出して実行することになる。

【００５１】具体的には、この制御部１０７では、大容量記憶媒体１０１上に保持した原本のコピーを作成した場合に、外部装置１１０からの要求に応答して証明書発行部１０６に対して保存証明書の発行を指示し、この証明書発行部１０６により発行された保存証明書を外部装置１１０に送信する。これにより、外部装置１１０は、この保存証明書を用いて複写データの正当性を検証することができる。

【００５２】つぎに、外部装置１１０の構成について説明する。図１に示すように、この外部装置１１０は、通信ポート１１１と、記憶部１１２と、検証部１１３と、制御部１１４とからなる。

【００５３】通信ポート１１１は、ネットワークを介して原本性保証電子保存１００との通信をおこなうためのインターフェース部であり、記憶部１１２は、原本性保証電子保存装置１００からネットワーク通信により受け取った原本の複写データなどを記憶する記憶媒体であり、制御部１１４は、外部装置１１０の全体制御をおこなう制御部である。

【００５４】検証部１１３は、原本性保証電子保存装置１００から複写データとともに受け取った保存証明書に基づいて、この複写データの正当性すなわちこの複写データが大容量記憶媒体１０１上に保持した原本の保存データと一致するか否かを検証する処理部である。

【００５５】すなわち、この検証部１１３が、保存証明書に基づいて複写データの正当性を効率良く検証するので、この外部装置１１０上に原本を移動しなくとも、この複写データが大容量記憶媒体１０１上に保持した原本の保存データと一致するか否かを確認することができる。

【００５６】上記構成を有する原本性保証電子保存装置１００および外部装置１１０からなる正当性検証システムを用いることにより、原本の保存データを複写した複写データの正当性を外部装置１１０上で効率良く検証することができる。

【００５７】つぎに、図１に示した証明書発行部１０６による保存証明書の作成手順について説明する。図２は、図１に示した証明書発行部１０６による保存証明書の作成手順を示すフローチャートであり、また、図３は、図１に示した証明書発行部１０６による保存証明書の作成概念を説明するための説明図である。

【００５８】図２および図３に示すように、この証明書発行部１０６は、外部装置１１０から保存証明書取得要求とともに、保存証明書の取得対象となる保存データの保存データ識別番号を受け付けたならば、後述する最新バージョン正当性検証処理をおこない（ステップＳ２０１～Ｓ２０２）、正当性の検証に失敗したならば（ステップＳ２０２否定）、エラー処理（ステップＳ２１１）の後に処理を終了する。

【００５９】これに対して、正当性の検証を成功した場合（ステップＳ２０２肯定）には、データ属性情報ファイル３０１と最新バージョンのコンテンツファイル全体に対してハッシュ値を計算してファイルハッシュ値３０８とする（ステップＳ２０３）。

【００６０】図３の例においては、保存データ３００が、データ属性情報ファイル３０１と、データアクセス履歴ファイル３０２と、データ認証ファイル３０３と、バージョン１情報３０４と、バージョン２情報３０５と、バージョン３情報３０６とからなるので、このデータ属性情報ファイル３０１および最新バージョンのコンテンツファイルを合わせたデータ３０７についてハッシュ値を計算して、これをファイルハッシュ値３０８としている。

【００６１】そして、このファイルハッシュ値３０８、内部タイマ１０５から取得した現在の日時情報（保存証明取得日時情報）、装置復号鍵（装置公開鍵）および保存データ識別番号を合わせて保存証明内容３０９とする

（ステップＳ２０４）。

【００６２】また、この保存証明内容３０９に対してハッシュ値を計算し、これを保存証明内容ハッシュ値３１０とし（ステップＳ２０５）、この保存証明内容ハッシュ値３１０を装置暗号鍵（装置秘密鍵）で暗号化して、これを保存証明内容署名３１１とする（ステップＳ２０６）。そして、先の保存証明内容３０９に保存証明内容署名を３１１付与して保存証明書とし（ステップＳ２０７）、この保存証明書を外部装置１１０に送出する（ステップＳ２０８）。

【００６３】なお、コンテンツ取得フラグが真（ＴＲＵＥ）であり、コンテンツの要求がなされている場合（ステップＳ２０９肯定）には、データ属性情報ファイルと最新バージョンのコンテンツファイルとを外部装置に送出した後に（ステップＳ２１０）処理を終了する。

【００６４】上記一連の処理をおこなうことにより、複写データの正当性を検証するための保存証明書を作成し、該作成した保存証明書を外部装置１１０に送信することができる。

【００６５】つぎに、図１に示した検証部１１３による保存証明書の検証処理について説明する。図４は、図１に示した検証部１１３による保存証明書の検証処理手順を示すフローチャートである。

【００６６】同図に示すように、まず最初に保存証明書から保存証明内容署名並びに装置公開鍵証明書を取り出して（ステップＳ４０１～Ｓ４０２）、この装置公開鍵証明書を検証し（ステップＳ４０３）、装置公開鍵証明書の検証に失敗したならば（ステップＳ４０４否定）、公開鍵証明書の正当性の確認ができないことをユーザに警告し（ステップＳ４０５）、エラー処理をおこなった後に（ステップＳ４１５）処理を終了する。

【００６７】これに対して、装置公開鍵証明書の検証に成功したならば（ステップＳ４０４肯定）、この装置公開鍵で保存証明内容署名を復号し（ステップＳ４０６）、保存証明書の保存証明内容部分についてハッシュ値を計算する（ステップＳ４０７）。

【００６８】そして、計算したハッシュ値と先に復号した保存内容署名とを比較し（ステップＳ４０８）、両者が一致しない場合（ステップＳ４０８否定）には、保存証明書が壊れていることをユーザに警告し（ステップＳ４０９）、エラー処理をおこなった後に（ステップＳ４１５）処理を終了する。

【００６９】一方、両者が一致する場合（ステップＳ４０８肯定）には、保存証明書とともに保存してあるデータ属性情報ファイル、最新バージョンのコンテンツファイルすべてを合わせたもののハッシュ値を計算した後（ステップＳ４１０）、保存証明書からファイルハッシュ値を取り出す（ステップＳ４１１）。

【００７０】そして、計算したハッシュ値がファイルハッシュ値とを比較し（ステップＳ４１２）、両者が一致しない場合（ステップＳ４１２否定）には、保存証明書とともに保存してあるファイルが改変されていることをユーザに警告し（ステップＳ４１３）、エラー処理をおこなった後に（ステップＳ４１５）処理を終了する。

【００７１】これに対して、両者が一致する場合（ステップＳ４１２肯定）には、保存証明書の確認が成功した旨を保存証明書の日時情報とともにユーザに表示した後に（ステップＳ４１４）、処理を終了する。

【００７２】上記一連の処理をおこなうことにより、証明書発行部１０６により発行された保存証明書に基づいて、検証部１１３が複写データの正当性を検証することができる。

【００７３】ところで、上記検証部１１３がおこなう検証処理では、保存証明書の証明対象となるコンテンツに変更がない場合を示したが、場合によっては、原本性保証電子保存装置１００の内部においては、当該コンテンツが最新の状態でない状況も生じ得る。

【００７４】そこで、かかる場合には、外部装置１１０が原本性保証電子保存装置１００に対して保存証明書を提示することにより、保存証明書の正当性の検証と、その保存証明書が対象とするコンテンツが最新の状態であるか否かを確認できることとする。なお、かかる検証処理は、原本性保証電子保存装置１００の証明書発行部１０６によりおこなわれることとなる。

【００７５】図５は、図１に示した原本性保証電子保存装置１００がおこなう保存証明書の正当性の検証処理並びにその保存証明書が対象とするコンテンツが最新の状態であるか否かの確認処理手順を示すフローチャートである。

【００７６】同図に示すように、まず最初に、受け取った保存証明書から保存証明内容署名並びに装置公開鍵証明書を取り出し（ステップＳ５０１～Ｓ５０２）、この装置公開鍵証明書が内部記憶媒体１０４に記録されている装置公開鍵証明書と一致するか否かを確認し（ステップＳ５０３）、両者が一致しない場合（ステップＳ５０３否定）には、エラー処理をおこなった後に（ステップＳ５１８）処理を終了する。

【００７７】これに対して、両者が一致する場合（ステップＳ５０３肯定）には、装置公開鍵で保存証明内容署名を復号し（ステップＳ５０４）、保存証明書の保存証明内容部分についてハッシュ値を計算する（ステップＳ５０５）。

【００７８】そして、計算したハッシュ値と先に復号した保存証明内容署名が一致するか否かを確認し（ステップＳ５０６）、両者が一致しない場合（ステップＳ５０６否定）には、エラー処理をおこなった後に（ステップＳ５１８）処理を終了する。

【００７９】これに対して、両者が一致する場合（ステップＳ５０６肯定）には、保存証明書から保存データ識別番号を取得し（ステップＳ５０７）、この保存データ

識別番号を渡して後述する最新バージョンの正当性検証処理をおこない（ステップＳ５０８）、検証に失敗したならば（ステップＳ５０９否定）、エラー処理をおこなった後に（ステップＳ５１８）処理を終了する。

【００８０】これに対して、検証処理に成功したならば（ステップＳ５０９肯定）、保存証明書から保存証明書取得日時情報を取得し（ステップＳ５１０）、データ属性情報ファイルから最終更新日時情報を取得する（ステップＳ５１１）。

【００８１】そして、最新更新日時の方が保存証明書取得日時よりも後である場合（ステップＳ５１２肯定）には、更新されていることを示すステータスコード、最終更新日時情報を外部装置１１０に対して送出して（ステップＳ５１３）、処理を終了する。

【００８２】これに対して、最新更新日時が保存証明書取得日時よりも後ではない場合（ステップＳ５１２否定）には、読み出したデータ属性情報ファイル、最新バージョンのコンテンツファイルをすべて合わせたもののハッシュ値を計算し（ステップＳ５１４）、保存証明書からファイルハッシュ値を取り出し（ステップＳ５１５）、計算したハッシュ値がファイルハッシュ値と一致するか否かを確認する（ステップＳ５１６）。

【００８３】その結果、両者が一致しない場合（ステップＳ５１６否定）には、エラー処理をおこなった後に（ステップＳ５１８）処理を終了し、両者が一致する場合（ステップＳ５１６肯定）には、最新の状態であることを示すステータスコード、最終更新日時を外部装置１１０に送出して（ステップＳ５１７）、処理を終了する。

【００８４】上記一連の処理をおこなうことにより、保存証明書の正当性の検証と、その保存証明書が対象とするコンテンツが最新の状態であるか否かを確認することができる。

【００８５】つぎに、図２および図５に示した最新バージョンの正当性検証処理について具体的に説明する。図６は、図２および図５に示した最新バージョンの正当性検証処理手順を示すフローチャートである。

【００８６】同図に示すように、まず最初に大容量記憶媒体１０１から保存データリストファイルを読み出し（ステップＳ６０１）、保存データリストファイルに受け取った保存データ識別番号に該当する保存データエントリを取得し（ステップＳ６０２）、該当する保存データエントリが存在するか否かを確認する（ステップＳ６０３）。

【００８７】その結果、該当する保存データエントリが存在しない場合（ステップＳ６０３否定）には、エラー処理をおこなった後に（ステップＳ６１７）処理を終了し、該当する保存データエントリが存在する場合（ステップＳ６０３肯定）には、保存データエントリから保存データＭＡＣを取得するとともに（ステップＳ６０４）、保存データ識別番号に該当する保存データのデータ認証ファイルを大容量記憶媒体１０１から読み出し（ステップＳ６０５）、データ認証ファイルからハッシュリストＭＡＣを取り出す（ステップＳ６０６）。

【００８８】なお、この保存データＭＡＣおよびハッシュリストＭＡＣのＭＡＣとは、メッセージ認証子（Message Authentication Code）のことであり、内部記憶媒体１０４内に記憶した秘密鍵を用いて作成される。

【００８９】そして、このハッシュリストＭＡＣと保存データＭＡＣが一致するか否かを確認し（ステップＳ６０７）、両者が一致しない場合（ステップＳ６０７否定）には、エラー処理をおこなった（ステップＳ６１７）後に処理を終了し、両者が一致する場合（ステップＳ６０７肯定）には、ハッシュリストＭＡＣを装置暗号鍵（公開鍵）で復号してハッシュリストハッシュとし（ステップＳ６０８）、データ認証ファイルのハッシュリストＭＡＣ以外の部分のハッシュ値を計算する（ステップＳ６０９）。

【００９０】そして、計算したハッシュ値と先のハッシュ値が一致するか否かを確認し（ステップＳ６１０）、両者が一致しない場合（ステップＳ６１０否定）には、エラー処理をおこなった（ステップＳ６１７）後に処理を終了し、両者が一致する場合（ステップＳ６１０肯定）には、保存データ識別番号に該当する保存データの最新バージョンに相当するコンテンツファイルをすべて大容量記憶媒体１０１から読み出し（ステップＳ６１１）、読み出したコンテンツファイルについてそれぞれハッシュ値を計算する（ステップＳ６１２）。

【００９１】そして、計算したハッシュ値がデータ認証ファイル内の該当するハッシュ値と一致するか否かを確認し（ステップＳ６１３）、両者が一致しない場合（ステップＳ６１３否定）には、エラー処理をおこなった（ステップＳ６１７）後に処理を終了し、両者が一致する場合（ステップＳ６１３肯定）には、保存データ識別番号に該当する保存データのデータ属性情報ファイルを大容量記憶媒体１０１から読み出し（ステップＳ６１４）、読み出したデータ属性情報ファイルについてハッシュ値を計算する（ステップＳ６１５）。

【００９２】そして、計算したハッシュ値がデータ認証ファイル内の該当するハッシュ値と一致するか否かを確認し（ステップＳ６１６）、一致しない場合（ステップＳ６１６否定）には、エラー処理をおこなった後に（ステップＳ６１７）処理を終了し、一致する場合（ステップＳ６１６肯定）には、そのまま処理を終了する。

【００９３】上述してきたように、本実施の形態では、原本性保証電子保存装置１０６の証明書発行部１０６が原本をコピーした複写データについての保存証明書を発行し、外部装置１１０の検証部１１３が保存証明書に基づいて複写データの正当性を検証するよう構成したので、外部装置１１０上に原本のコピーを保持する場合

に、このコピーが原本の保存データと一致することを効率良く保証することができる。

【００９４】

【発明の効果】以上説明したように、請求項１に記載の発明によれば、複写データが原本データとその内容が一致することを証明する証明書を発行し、発行した証明書に基づいて複写データの正当性を検証することとしたので、原本性保証電子保存装置以外の装置上に原本のコピーを保持する場合に、このコピーが原本の保存データと一致することを効率良く保証することができる正当性検証システムが得られるという効果を奏する。

【００９５】また、請求項２に記載の発明によれば、記憶部に記憶した原本データについての第１のハッシュ値を算定し、算定した第１のハッシュ値を所定の秘密鍵で暗号化し、暗号化した暗号データを証明書として出力することとしたので、迅速かつ効率良く証明書を発行することができる正当性検証システムが得られるという効果を奏する。

【００９６】また、請求項３に記載の発明によれば、原本データについての第１のハッシュ値を算定し、算定した第１のハッシュ値、現在時刻および原本データの識別情報を含む証明内容を作成し、作成した証明内容についての第２のハッシュ値を算定し、算定した第２のハッシュ値並びに証明内容からなる証明書を出力することとしたので、２重にハッシュ化した高い正当性を保証することができる証明書を発行することができる正当性検証システムが得られるという効果を奏する。

【００９７】また、請求項４に記載の発明によれば、記憶部に記憶した原本データの最新版の内容データとその属性情報についての第１のハッシュ値を算定することとしたので、正当性を保証すべき内容のみに限定した保証書を効率良く発行することができる正当性検証システムが得られるという効果を奏する。

【００９８】また、請求項５に記載の発明によれば、発行された証明書とともに検証要求を受け付けた際に、当該証明書を秘密鍵に対応する公開鍵で復号化するとともに、記憶部に記憶した原本データのハッシュ値を算定し、算定したハッシュ値および復号化された値を比較して、両者が一致する場合にのみ複写データが正当であるものと判定することとしたので、迅速かつ効率良く複写データの正当性を検証することができる正当性検証システムが得られるという効果を奏する。

【００９９】また、請求項６に記載の発明によれば、証明書に含まれる第２のハッシュ値を秘密鍵に対応する公開鍵で復号化するとともに、証明書に含まれる証明内容についての第３のハッシュ値を算定し、この復号化された第２のハッシュ値および算定された第３のハッシュ値が一致する場合に、証明内容に含まれる識別情報に対応する原本データを記憶部から読み出し、読み出した原本データについての第４のハッシュ値を算定し、算定した第４のハッシュ値および証明内容に含まれる第１のハッシュ値を比較して、両者が一致する場合にのみ複写データが正当であるものと判定することとしたので、より確実に複写データが正当なものであるか否かを検証することができる正当性検証システムが得られるという効果を奏する。

【０１００】また、請求項７に記載の発明によれば、読み出された原本データの最新版の内容データとその属性情報についての第４のハッシュ値を算定することとしたので、検証時間の短縮化を図ることができる正当性検証システムが得られるという効果を奏する。

【０１０１】また、請求項８に記載の発明によれば、複写データが原本データとその内容が一致することを証明する証明書を発行し、発行した証明書に基づいて複写データの正当性を検証することとしたので、原本性保証電子保存装置以外の装置上に原本のコピーを保持する場合に、このコピーが原本の保存データと一致することを効率良く保証することができる正当性検証方法が得られるという効果を奏する。

【０１０２】また、請求項９に記載の発明によれば、記憶部に記憶した原本データについての第１のハッシュ値を算定し、算定した第１のハッシュ値を所定の秘密鍵で暗号化し、暗号化した暗号データを証明書として出力することとしたので、迅速かつ効率良く証明書を発行することができる正当性検証方法が得られるという効果を奏する。

【０１０３】また、請求項１０に記載の発明によれば、原本データについての第１のハッシュ値を算定し、算定した第１のハッシュ値、現在時刻および原本データの識別情報を含む証明内容を作成し、作成した証明内容についての第２のハッシュ値を算定し、算定した第２のハッシュ値並びに証明内容からなる証明書を出力することとしたので、２重にハッシュ化した高い正当性を保証することができる証明書を発行することができる正当性検証方法が得られるという効果を奏する。

【０１０４】また、請求項１１に記載の発明によれば、記憶部に記憶した原本データの最新版の内容データとその属性情報についての第１のハッシュ値を算定することとしたので、正当性を保証すべき内容のみに限定した保証書を効率良く発行することができる正当性検証方法が得られるという効果を奏する。

【０１０５】また、請求項１２に記載の発明によれば、発行された証明書とともに検証要求を受け付けた際に、当該証明書を秘密鍵に対応する公開鍵で復号化するとともに、記憶部に記憶した原本データのハッシュ値を算定し、算定したハッシュ値および復号化された値を比較して、両者が一致する場合にのみ複写データが正当であるものと判定することとしたので、迅速かつ効率良く複写データの正当性を検証することができる正当性検証方法が得られるという効果を奏する。

19

【０１０６】また、請求項１３に記載の発明によれば、証明書に含まれる第２のハッシュ値を秘密鍵に対応する公開鍵で復号化するとともに、証明書に含まれる証明内容についての第３のハッシュ値を算定し、この復号化された第２のハッシュ値および算定された第３のハッシュ値が一致する場合に、証明内容に含まれる識別情報に対応する原本データを記憶部から読み出し、読み出した原本データについての第４のハッシュ値を算定し、算定した第４のハッシュ値および証明内容に含まれる第１のハッシュ値を比較して、両者が一致する場合にのみ複写データが正当であるものと判定することとしたので、より確実に複写データが正当なものであるか否かを検証することができる正当性検証方法が得られるという効果を奏する。

【０１０７】また、請求項１４に記載の発明によれば、読み出された原本データの最新版の内容データとその属性情報についての第４のハッシュ値を算定することとしたので、検証時間の短縮化を図ることができる正当性検証方法が得られるという効果を奏する。

【０１０８】また、請求項１５に記載の発明にかかる記録媒体は、請求項８～１４のいずれか一つに記載された方法をコンピュータに実行させるプログラムを記録したことで、そのプログラムが機械読み取り可能となり、これによって、請求項８～１４の動作をコンピュータによって実現することができる。

【図面の簡単な説明】

【図１】この実施の形態で用いる正当性検証システムの

20

システム構成を示すブロック図である。

【図２】図１に示した証明書発行部による保存証明書の作成手順を示すフローチャートである。

【図３】図１に示した証明書発行部による保存証明書の作成概念を説明するための説明図である。

【図４】図１に示した検証部による保存証明書の検証処理手順を示すフローチャートである。

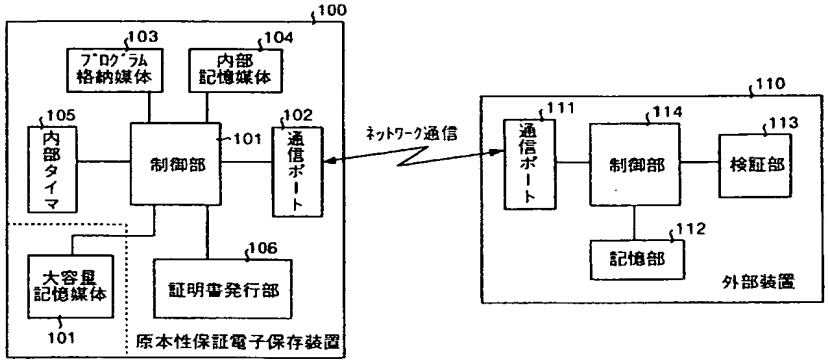
【図５】図１に示した原本性保証電子保存装置がおこなう保存証明書の正当性の検証処理並びにその保存証明書が対象とするコンテンツが最新の状態であるか否かの確認処理手順を示すフローチャートである。

【図６】図２および図５に示した最新バージョンの正当性検証処理手順を示すフローチャートである。

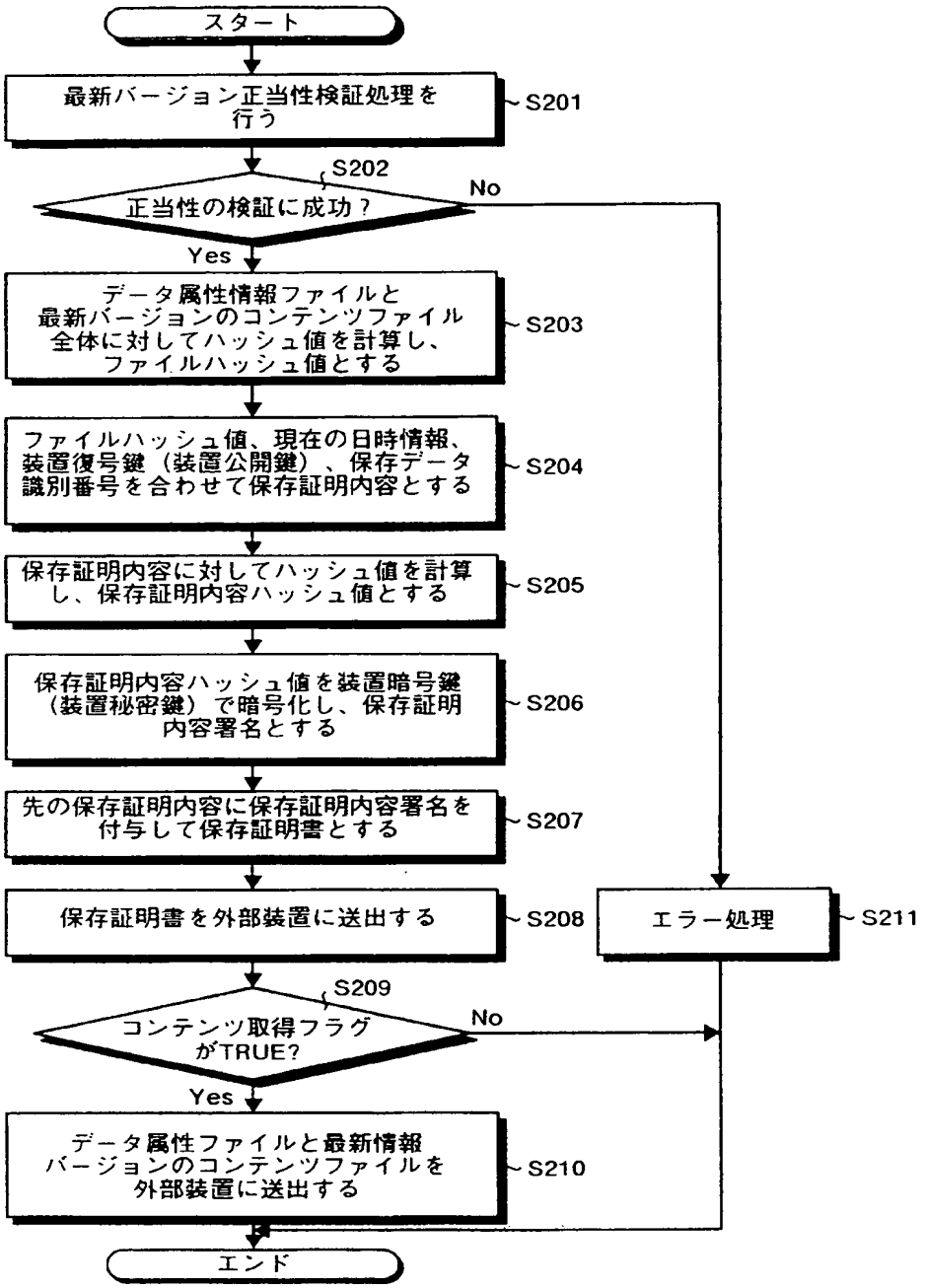
【符号の説明】

１００　原本性保証電子保存装置
１０１　大容量記憶媒体
１０２　通信ポート
１０３　プログラム格納媒体
１０４　内部記録媒体
１０５　内部タイマ
１０６　証明書発行部
１０７　制御部
１１０　外部装置
１１１　通信ポート
１１２　記憶部
１１３　検証部
１１４　制御部

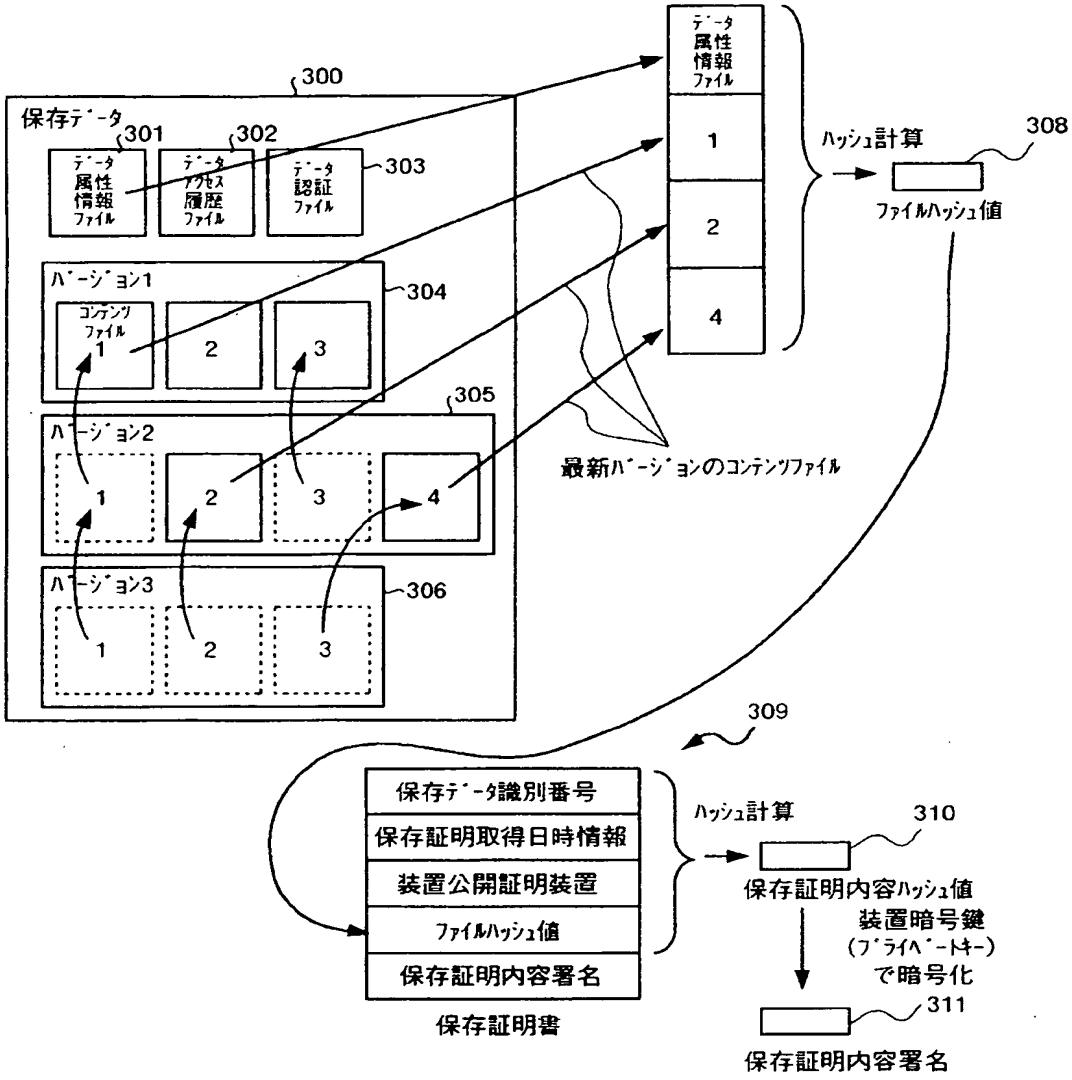
【図１】



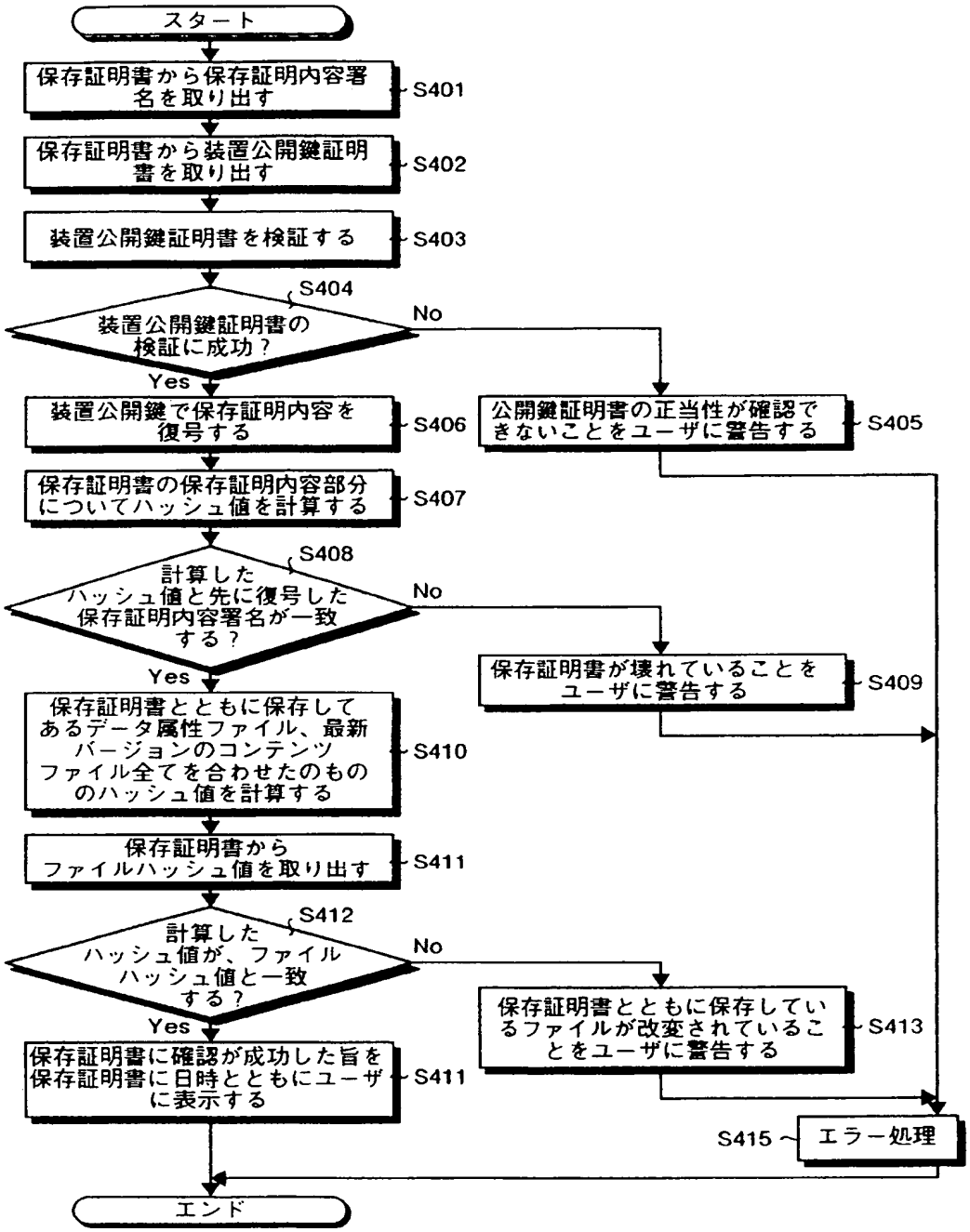
【図２】


スタート
最新バージョン正当性検証処理を行う
S201
S202
正当性の検証に成功？
No
Yes
データ属性情報ファイルと最新バージョンのコンテンツファイル全体に対してハッシュ値を計算し、ファイルハッシュ値とする
S203
ファイルハッシュ値、現在の日時情報、装置復号鍵（装置公開鍵）、保存データ識別番号を合わせて保存証明内容とする
S204
保存証明内容に対してハッシュ値を計算し、保存証明内容ハッシュ値とする
S205
保存証明内容ハッシュ値を装置暗号鍵（装置秘密鍵）で暗号化し、保存証明内容署名とする
S206
先の保存証明内容に保存証明内容署名を付与して保存証明書とする
S207
保存証明書を外部装置に送出する
S208
エラー処理
S211
S209
コンテンツ取得フラグがTRUE?
No
Yes
データ属性ファイルと最新情報バージョンのコンテンツファイルを外部装置に送出する
S210
エンド

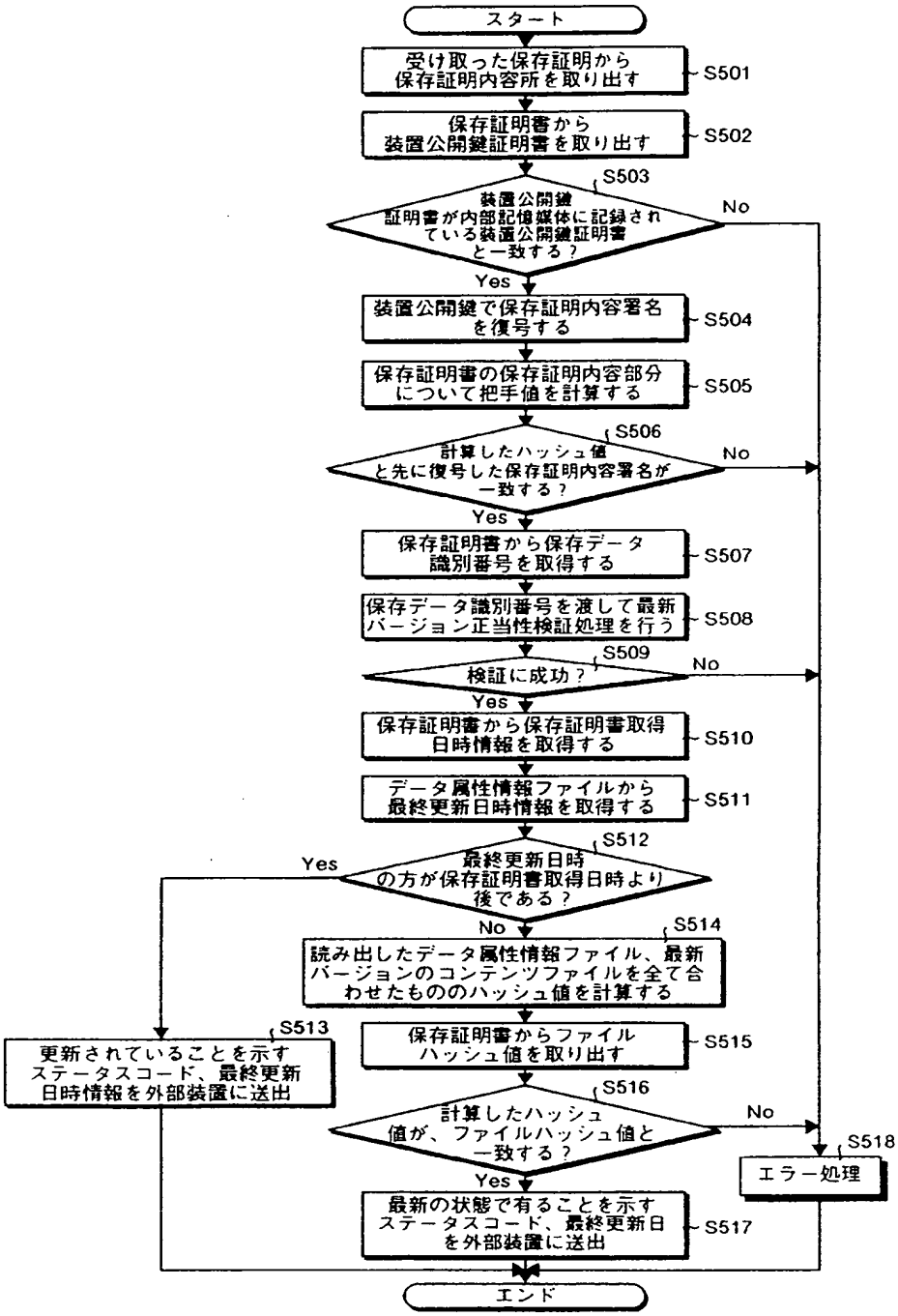
【図３】


300
保存ﾃﾞｰﾀ
301
302
303
ﾃﾞｰﾀ 属性情報 ファイル
ﾃﾞｰﾀ アクセス履歴 ファイル
ﾃﾞｰﾀ 認証 ファイル
ﾊﾞｰｼﾞｮﾝ1
304
ｺﾝﾃﾝﾂ ファイル
1
2
3
ﾊﾞｰｼﾞｮﾝ2
305
ﾊﾞｰｼﾞｮﾝ3
306
ﾃﾞｰﾀ 属性情報 ファイル
1
2
4
最新ﾊﾞｰｼﾞｮﾝのｺﾝﾃﾝﾂﾌｧｲﾙ
ﾊｯｼｭ計算
308
ﾌｧｲﾙﾊｯｼｭ値
309
保存ﾃﾞｰﾀ識別番号
保存証明取得日時情報
装置公開証明装置
ﾌｧｲﾙﾊｯｼｭ値
保存証明内容署名
保存証明書
ﾊｯｼｭ計算
310
保存証明内容ﾊｯｼｭ値
装置暗号鍵
(ﾌﾟﾗｲﾍﾞｰﾄｷｰ)
で暗号化
311
保存証明内容署名

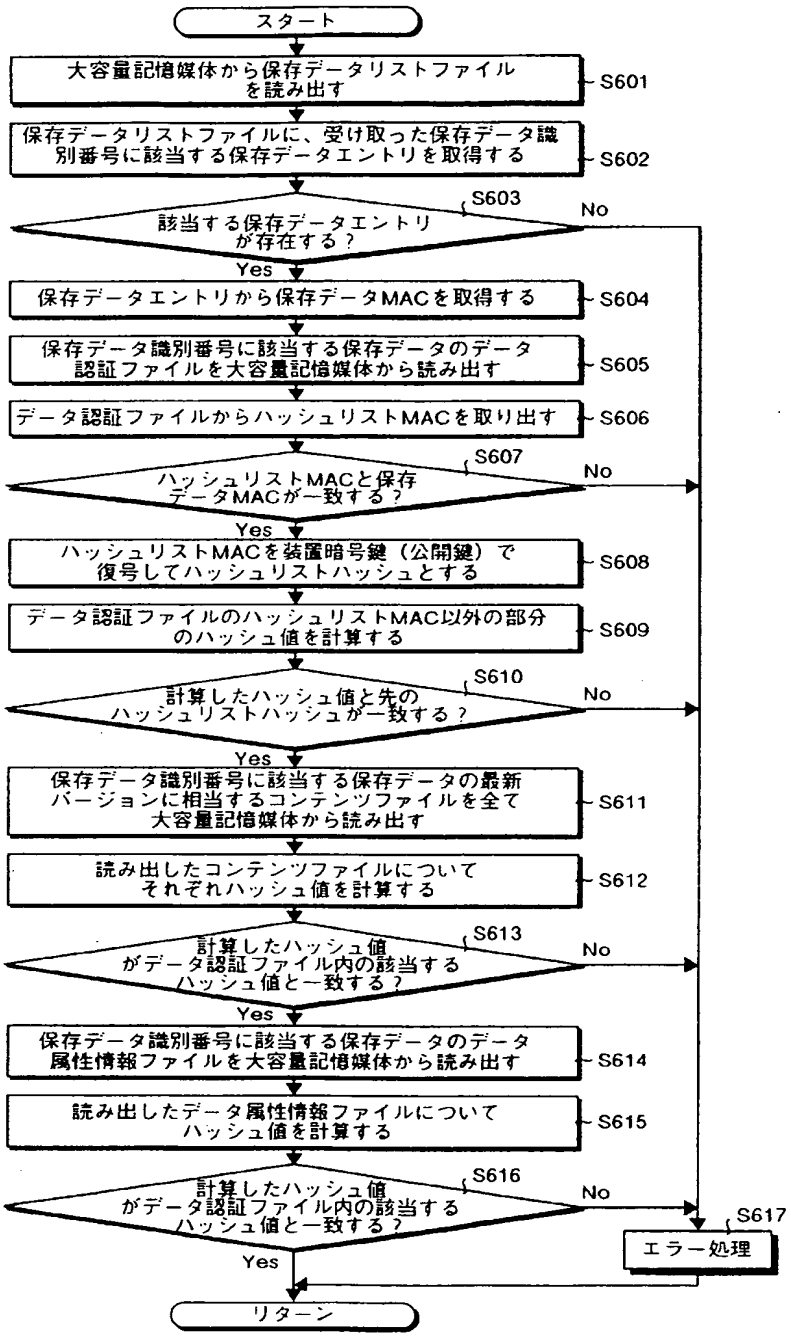
【図４】


スタート
保存証明書から保存証明内容署名を取り出す
S401
保存証明書から装置公開鍵証明書を取り出す
S402
装置公開鍵証明書を検証する
S403
S404
装置公開鍵証明書の検証に成功？
No
Yes
装置公開鍵で保存証明内容を復号する
S406
公開鍵証明書の正当性が確認できないことをユーザに警告する
S405
保存証明書の保存証明内容部分についてハッシュ値を計算する
S407
S408
計算したハッシュ値と先に復号した保存証明内容署名が一致する？
No
Yes
保存証明書が壊れていることをユーザに警告する
S409
保存証明書とともに保存してあるデータ属性ファイル、最新バージョンのコンテンツファイル全てを合わせたもののハッシュ値を計算する
S410
保存証明書からファイルハッシュ値を取り出す
S411
S412
計算したハッシュ値が、ファイルハッシュ値と一致する？
No
Yes
保存証明書とともに保存しているファイルが改変されていることをユーザに警告する
S413
保存証明書に確認が成功した旨を保存証明書に日時とともにユーザに表示する
S411
S415
エラー処理
エンド

【図５】


スタート
受け取った保存証明から保存証明内容所を取り出す
S501
保存証明書から装置公開鍵証明書を取り出す
S502
S503
装置公開鍵証明書が内部記憶媒体に記録されている装置公開鍵証明書と一致する？
No
Yes
装置公開鍵で保存証明内容署名を復号する
S504
保存証明書の保存証明内容部分について把手値を計算する
S505
S506
計算したハッシュ値と先に復号した保存証明内容署名が一致する？
No
Yes
保存証明書から保存データ識別番号を取得する
S507
保存データ識別番号を渡して最新バージョン正当性検証処理を行う
S508
S509
検証に成功？
No
Yes
保存証明書から保存証明書取得日時情報を取得する
S510
データ属性情報ファイルから最終更新日時情報を取得する
S511
S512
最終更新日時の方が保存証明書取得日時より後である？
Yes
No
S514
読み出したデータ属性情報ファイル、最新バージョンのコンテンツファイルを全て合わせたもののハッシュ値を計算する
S513
更新されていることを示すステータスコード、最終更新日時情報を外部装置に送出
保存証明書からファイルハッシュ値を取り出す
S515
S516
計算したハッシュ値が、ファイルハッシュ値と一致する？
No
Yes
S518
エラー処理
最新の状態で有ることを示すステータスコード、最終更新日を外部装置に送出
S517
エンド

【図６】


スタート
大容量記憶媒体から保存データリストファイルを読み出す
S601
保存データリストファイルに、受け取った保存データ識別番号に該当する保存データエントリを取得する
S602
S603
該当する保存データエントリが存在する？
No
Yes
保存データエントリから保存データMACを取得する
S604
保存データ識別番号に該当する保存データのデータ認証ファイルを大容量記憶媒体から読み出す
S605
データ認証ファイルからハッシュリストMACを取り出す
S606
S607
ハッシュリストMACと保存データMACが一致する？
No
Yes
ハッシュリストMACを装置暗号鍵（公開鍵）で復号してハッシュリストハッシュとする
S608
データ認証ファイルのハッシュリストMAC以外の部分のハッシュ値を計算する
S609
S610
計算したハッシュ値と先のハッシュリストハッシュが一致する？
No
Yes
保存データ識別番号に該当する保存データの最新バージョンに相当するコンテンツファイルを全て大容量記憶媒体から読み出す
S611
読み出したコンテンツファイルについてそれぞれハッシュ値を計算する
S612
S613
計算したハッシュ値がデータ認証ファイル内の該当するハッシュ値と一致する？
No
Yes
保存データ識別番号に該当する保存データのデータ属性情報ファイルを大容量記憶媒体から読み出す
S614
読み出したデータ属性情報ファイルについてハッシュ値を計算する
S615
S616
計算したハッシュ値がデータ認証ファイル内の該当するハッシュ値と一致する？
No
Yes
S617
エラー処理
リターン